566.40596X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: T. FUJISHIRO, et al

Serial No.: 09/941,771

Filing Date: August 30, 2001

For: CERTIFICATE VALIDITY AUTHENTICATION METHOD AND APPARATUS

Attention: Box Missing Parts

LETTER CLAIMING RIGHT OF PRIORITY

Assistant Commissioner
for Patents
Washington, D.C. 20231

January 2, 2002

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, applicants hereby claim the right of priority based on:

Japanese Application No. 2000-261065
Filed: August 30, 2000

A Certified Copy of said application documents are attached hereto.

Respectfully submitted,

Carl I. Brundidge
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP

CIB/jdc
Enclosures
703/312-6600

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　８月３０日

出願番号
Application Number: 特願２０００－２６１０６５

出願人
Applicant(s): 株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　８月３１日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

【書類名】　特許願

【整理番号】　HK13379000

【提出日】　平成12年 8月30日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 9/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　藤城　孝宏

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　手塚　悟

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　熊谷　洋子

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共情報事業部内

【氏名】　森尾　智治

【発明者】

【住所又は居所】　東京都江東区新砂一丁目６番２７号　株式会社日立製作所　公共情報事業部内

【氏名】　宮崎　豊

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100087170

【弁理士】

【氏名又は名称】　富田　和子

【電話番号】　045(316)3711

【手数料の表示】

【予納台帳番号】　012014

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】証明書の有効性確認方法および装置

【特許請求の範囲】

【請求項１】

端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認する証明書の有効性確認方法であって、

任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索ステップと、

前記パス検索ステップにより検出されたパスについて、前記起点認証局を上流とし、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を１つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該１つ上流側の認証局が発行した公開鍵証明書の署名をさらに１つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該１つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証ステップと、

前記パス検証ステップにより検証が成立したパスをデータベースに登録するパス登録ステップと、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているときに、前記公開鍵証明書の有効性が確認されたものと判断する有効性確認ステップと、を有すること

を特徴とする証明書の有効性確認方法。

【請求項２】

請求項１記載の証明書の有効性確認方法であって、

前記パス検索ステップは、定期的に実行され、

前記パス検証ステップは、前記パス検索ステップにより検索された最新のパス

に対して実行され、そして、

前記パス登録ステップは、前記データベースの登録内容を、前記パス検証ステップで検証が成立した最新のパスに更新すること

を特徴とする証明書の有効性確認方法。

【請求項３】

請求項１または２記載の証明書の有効性確認方法であって、

前記パス登録ステップにより前記データベースに登録されている各パスについて、当該パス上の各認証局が発行した１つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書各々の有効期限を調べる有効期限調査ステップと、

前記有効期限調査ステップにより有効期限を過ぎていることが確認された公開鍵証明書の発行元から、当該公開鍵証明書の発行先に対する新たな公開鍵証明書を入手し、少なくとも、当該新たな公開鍵証明書の署名を、前記発行元より１つ上流側の認証局が発行した公開鍵証明書で検証するパス再検証ステップと、をさらに有し、

前記パス登録ステップは、

前記パス再検証ステップにて前記新たな公開鍵証明書の署名検証が成立しなかった場合、あるいは、前記新たな公開鍵証明書を入手できなかった場合は、前記有効期限調査ステップにより有効期限を過ぎていることが確認された公開鍵証明書の発行元と発行先とを含むパスを、前記データベースから削除すること

を特徴とする証明書の有効性確認方法。

【請求項４】

請求項１、２または３記載の証明書の有効性確認方法であって、

前記パス登録ステップにより前記データベースに登録されている各パスについて、当該パス上の各認証局が発行した公開鍵証明書の失効情報を調査する失効情報調査ステップをさらに有し、

前記パス登録ステップは、

前記失効情報調査ステップにより失効していることが確認された公開鍵証明書の発行元と発行先とを含むパスが前記データベースに登録されている場合は、こ

れを前記データベースから削除すること

を特徴とする証明書の有効性確認方法。

【請求項５】

請求項１、２、３または４記載の証明書の有効性確認方法であって、

前記有効性確認ステップは、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されている場合でも、この２つのパス上のいずれかの認証局が発行した、当該認証局が位置するパス上の１つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書中に、前記２つのパス上のいずれかの認証局を信頼しない旨の制限が記述されている場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること

を特徴とする証明書の有効性確認方法。

【請求項６】

請求項１、２、３、４または５記載の証明書の有効性確認方法であって、

前記有効性確認ステップは、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されている場合でも、この２つのパス上のいずれかの認証局が発行した、当該認証局が位置するパス上の１つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書中に記述されているパス長（パス上の許容最大認証局数）を、前記２つのパス上の認証局の合計数が超えている場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること

を特徴とする証明書の有効性確認方法。

【請求項７】

請求項１、２、３、４、５または６記載の証明書の有効性確認方法であって、

前記有効性確認ステップは、

端末から、当該端末が行おうとしている電子手続に要求される信頼度の提示を伴った、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されている場合でも、この２つのパス上のいずれかの認証局が発行した、当該認証局が位置するパス上の１つ下流側の認証局（発行元が端末収容認証局の場合は、当該認証局が収容する端末）に対する公開鍵証明書中に記述されている信頼度（ポリシー）が、前記電子手続に要求される信頼度よりも低い場合は、前記公開鍵証明書の有効性が確認されなかったものと判断すること

を特徴とする証明書の有効性確認方法。

【請求項８】

請求項１、２、３、４、５、６または７記載の証明書の有効性確認方法であって、

前記起点認証局は、

少なくとも２つのセキュリティドメインのルート認証局各々と相互認証を行っているブリッジ認証局であること

を特徴とする証明書の有効性確認方法。

【請求項９】

端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認する証明書の有効性確認装置であって、

任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索手段と、

前記パス検索手段により検出されたパスについて、前記起点認証局を上流とし

、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を１つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該１つ上流側の認証局が発行した公開鍵証明書の署名をさらに１つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該１つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証手段と、

前記パス検証手段により検証が成立したパスをデータベースに登録するパス登録手段と、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているときに、前記公開鍵証明書の有効性が確認されたものと判断する有効性確認手段と、を有すること

を特徴とする証明書の有効性確認装置。

【請求項１０】

端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認するためのプログラムが記憶された記憶媒体であって、

前記プログラムは、電子計算機に読み取られて実行されることで、

任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索手段と、

前記パス検索手段により検出されたパスについて、前記起点認証局を上流とし、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を１つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該１つ上流側の認証局が発行した公開鍵証明書の署名をさらに１つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該１つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証手段と、

前記パス検証手段により検証が成立したパスをデータベースに登録するパス登録手段と、

端末から、当該端末が信頼する認証局とは異なる端末収容認証局が発行した公開鍵証明書の有効性確認依頼があった場合、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているときに、前記公開鍵証明書の有効性が確認されたものと判断する有効性確認手段とを、当該電子計算機上に構築すること

を特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＰＫＩ（Public Key Infrastructure）において、ある端末が受け取った電子手続に対する署名を検証するための公開鍵証明書が、当該端末が信頼する認証局とは異なる認証局が発行したものである場合に、その有効性を確認するのに好適な技術に関する。

【０００２】

【従来の技術】

民間系、公共系の様々な組織、団体において、従来、紙面で行ってきた様々な手続を電子化するべく、ＰＫＩ（Public Key Infrastructure）の導入、整備が進んでいる。

【０００３】

図１２は、従来のＰＫＩにおいて、認証局が複数ある場合における各認証局の関係を示している。

【０００４】

図示するように、公開鍵証明書の発行とその管理を行う各認証局は、ルート認証局ＣＡ１を頂点とするツリー構造を持つグループを形成している。このグループはセキュリティドメインと呼ばれている。ルート認証局ＣＡ１は、自身より１つ下流側に位置する各認証局$CA2_1$～$CA2_n$に対して公開鍵証明書を発行する

。また、認証局ＣＡ２$_1$～ＣＡ２$_{n1}$各々は、自身より１つ下流側に位置する各認証局ＣＡ３$_1$～ＣＡ３$_{n2}$に対して公開鍵証明書を発行する。このように、ツリー上、１つ上流側に位置する認証局が自身より１つ下流側に位置する認証局に対して公開鍵証明書を発行する。そして、ツリー上、最下流に位置する認証局（以下、端末収容認証局と呼ぶ）ＣＡＳ$_1$～ＣＡＳ$_{nm}$は、電子手続を行うユーザ端末（以下、エンドエンティティと呼ぶ）ＥＥ$_1$～ＥＥ$_x$に対して公開鍵証明書を発行する。

【０００５】

エンドエンティティＥＥ$_1$～ＥＥ$_x$各々が電子文書の署名に使用する秘密鍵（署名鍵）の正当性は、自身を収容する端末収容認証局ＣＡＳ$_1$～ＣＡＳ$_{nm}$が発行した公開鍵証明書によって証明され、端末収容認証局ＣＡＳ$_1$～ＣＡＳ$_{nm}$各々が発行する公開鍵証明書の署名に使用する秘密鍵の正当性は、自身を収容する認証局ＣＡ（Ｓ－１）$_1$～ＣＡ（Ｓ－１）$_{n(m-1)}$が発行した公開鍵証明書によって証明される。したがって、エンドエンティティＥＥ$_1$～ＥＥ$_x$各々が署名に使用する秘密鍵は、最終的に、ルート認証局ＣＡ１が発行する公開鍵証明書によって証明されることになる。このエンドエンティティＥＥ$_1$～ＥＥ$_x$が署名に使用する鍵の正当性を最終的に証明する認証局、云いかえれば、エンドエンティティＥＥ$_1$～ＥＥ$_x$が信頼する、ツリー上、最上流側の認証局をトラストアンカーと呼ぶ。

【０００６】

さて、図１２において、エンドエンティティＥＥ$_1$は、エンドエンティティＥＥ$_x$に送信すべき申請書等の電子文書に対して、エンドエンティティＥＥ$_1$が保持する自身の秘密鍵で署名を行う。そして、署名した電子文書に、エンドエンティティＥＥ$_1$を収容する端末収容認証局ＣＡＳ$_1$が発行した前記秘密鍵と対の公開鍵証明書を添付して、エンドエンティティＥＥ$_x$に送信する。

【０００７】

エンドエンティティＥＥ$_x$は、エンドエンティティＥＥ$_1$より受け取った電子文書の署名を、当該電子文書に添付された公開鍵証明書を用いて検証することができる。しかし、公開鍵証明書はエンドエンティティＥＥ$_x$を収容する端末収容認証局ＣＡＳ$_{nm}$が発行したものではないので、エンドエンティティＥＥ$_x$は、当該

公開鍵証明書を直ちに信頼することはできない。この場合、エンドエンティティＥＥ$_x$は、自身のトラストアンカーであるルート認証局ＣＡ１によって当該公開鍵証明書の有効性が証明されるものであることを確認しなければならない。この公開鍵証明書の有効性確認処理は、以下の手順によって行われる。

【０００８】

①トラストアンカーから公開鍵証明書の発行元認証局までのパスの検索

トラストアンカー（ここでは、ルート認証局ＣＡ１）を起点認証局とし、起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先に、公開鍵証明書の発行元認証局（ここでは、エンドエンティティＥＥ$_1$を収容する端末収容認証局ＣＡＳ$_1$）が含まれるまで続け、トラストアンカーから公開鍵証明書の発行元認証局までのパスを検索する。

【０００９】

②検出したパスの検証

上記①により検出したパス上の各認証局から、パス上において当該認証局の１つ下流側の認証局に対して発行した公開鍵証明書を入手する。そして、有効性確認対象の公開鍵証明書（ここでは、端末収容認証局ＣＡＳ$_1$がエンドエンティティＥＥ$_1$に対して発行した公開鍵証明書）の署名を、当該公開鍵証明書を発行した認証局（ここでは、端末収容認証局ＣＡＳ$_1$）より１つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は、当該１つ上流側の認証局が発行した公開鍵証明書の署名をさらに１つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該１つ上流側の認証局がトラストアンカーとなるまで続ける。そして、このような公開鍵証明書の署名検証がトラストアンカーまで成立した場合に、有効性確認対象の公開鍵証明書の有効性が確認されたものとする。

【００１０】

エンドエンティティＥＥ$_x$は、エンドエンティティＥＥ$_1$より受け取った電子文書の署名を当該電子文書に添付された公開鍵証明書を用いて検証すると共に、上記の①、②に示す手順に従い当該電子文書の署名検証に用いた公開鍵証明書の有効性を確認することにより、当該電子文書の正当性を確認することができる。

【００１１】

なお、以上では、公開鍵証明書の有効性確認処理をエンドエンティティで行うことを前提としている。しかし、公開鍵証明書の有効性確認処理は負荷が重く、これをエンドエンティティで行うためには、当該エンドエンティティに高い処理能力が要求される。そこで、ネットワークを介してエンドエンティティに接続された証明書の有効性確認サーバを設け、当該サーバに、当該エンドエンティティの代わりに公開鍵証明書の有効性確認を行わせることがＩＥＴＦにより提案されている。

【００１２】

【発明が解決しようとする課題】

ところで、従来提案されている証明書の有効性確認サーバは、エンドエンティティから依頼を受ける都度、上記の①、②に示す手順を実行して公開鍵証明書の有効性を確認している。このため、エンドエンティティが公開鍵証明書の有効性確認を依頼をしてからその結果がわかるまでに、少なくとも、上記の①、②に示す手順を実行するための時間がかかってしまう。

【００１３】

なお、図１２では、セキュリティドメインが１つであることを前提にしているが、上述したように、民間系、公共系の様々な組織、団体においてＰＫＩの導入、整備が行われており、その結果、複数のセキュリティドメインが並存することが予想される。これらの異なるセキュリティドメイン間においても、各セキュリティドメインのルート認証局同士で、互いに相手の公開鍵証明書を発行するなどして相互認証を行ったり、あるいは、各セキュリティドメインのルート認証局各々との間でこのような相互認証を行ったブリッジ認証局を設置することにより、上記の①、②にその手順を示した公開鍵証明書の有効性確認処理を実現することができる。しかしこのように、複数のセキュリティドメイン間で公開鍵証明書の有効性確認処理を行うと、認証局数が増大し、また、各認証局の関係も、図１２に示すような単純なツリー構造ではなく、より複雑化するため、上記の①、②に示す手順を実行するための負荷が増大する。このため、エンドエンティティが公開鍵証明書の有効性確認を依頼をしてからその結果がわかるまでにかかる時間が

さらに長くなり、サービスの低下を招いてしまう。

【００１４】

本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短くすることにある。

【００１５】

【課題を解決するための手段】

上記課題を解決するために、本発明では、ネットワークを介して、複数の端末（エンドエンティティ）や認証局に接続された証明書の有効性確認サーバにおいて、ある端末からの依頼に応じて、当該端末が信頼する認証局とは異なる認証局が発行した公開鍵証明書の有効性を確認するために以下の処理を行う。

【００１６】

すなわち、任意の認証局を起点認証局とし、当該起点認証局が発行した公開鍵証明書の発行先を調べ、当該発行先に認証局が含まれる場合は当該認証局が発行した公開鍵証明書の発行先をさらに調べる処理を、当該公開鍵証明書の発行先が全て端末となるまで続けることにより、前記起点認証局から任意の端末に対して公開鍵証明書を発行した端末収容認証局までのパスを検索するパス検索ステップと、

前記パス検索ステップにより検出されたパスについて、前記起点認証局を上流とし、当該パス上の端末収容認証局が発行した公開鍵証明書の署名を１つ上流側の認証局が発行した公開鍵証明書で検証し、検証が成立した場合は当該１つ上流側の認証局が発行した公開鍵証明書の署名をさらに１つ上流側の認証局が発行した公開鍵証明書で検証する処理を、当該１つ上流側の認証局が前記起点認証局となるまで続けることにより、当該パスを検証するパス検証ステップと、

前記パス検証ステップにより検証が成立したパスをデータベースに登録するパス登録ステップとを、端末からの公開鍵証明書の有効性確認依頼とは無関係に、例えば定期的に行う。

【００１７】

そして、ある端末から、当該端末が信頼する認証局とは異なる端末収容認証局

が発行した公開鍵証明書の有効性確認依頼があった場合に、前記端末が信頼する認証局と前記起点認証局との間のパス、および、前記異なる端末収容認証局と前記起点認証局との間のパスが、前記データベースに登録されているか否かを調べることで、前記公開鍵証明書の有効性を確認する。

【００１８】

本発明によれば、ある端末から公開鍵証明書の有効性確認依頼を受けた場合に、それから、上記の①、②に示した、当該端末のトラストアンカーから当該公開鍵証明書の発行元認証局までのパスの検索、および、検出したパスの検証を行う必要がない。したがって、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮できる。

【００１９】

【発明の実施の形態】

以下に、本発明の一実施形態について説明する。

【００２０】

図１は、本発明の一実施形態が適用されたＰＫＩシステムの概略構成を示す図である。

【００２１】

図示するように、本実施形態のＰＫＩシステムは、電子手続を行うユーザ端末あるいはユーザ端末からの依頼を受けて電子手続を代行する受付サーバである複数のエンドエンティティＥＥと、公開鍵証明書の発行とその管理を行う複数の認証局ＣＡと、エンドエンティティＥＥからの依頼に応じ公開鍵証明書の有効性の確認を行う証明書有効性確認センタＶＣとが、ＬＡＮ、ＷＡＮおよびこれらを繋ぐインターネット等により構成されたネットワークＮＥＴを介して、互いに接続されて構成される。

【００２２】

図２は、図１に示すＰＫＩシステムでの各認証局ＣＡの関係の一例を示す図である。

【００２３】

図示するように、本実施形態のＰＫＩシステムでは、民間系、政府系といった

複数のセキュリティドメインＳＤ（SD_1～SD_3）が並存していることを前提としている。そして、そのうちの幾つかのセキュリティドメインＳＤ（図２ではSD_2、SD_3）は、ルート認証局ＣＡ（図２ではCA_{21}、CA_{31}）同士で、例えば互いに公開鍵証明書を発行し合うことにより相互認証を行っているものとする。また、各セキュリティドメインＳＤのルート認証局ＣＡ（図２ではCA_{11}、CA_{21}、CA_{31}）は、例えば、ブリッジ認証局CA_{bridge}に対して公開鍵証明書を発行すると共に、ブリッジ認証局CA_{bridge}から公開鍵証明書を発行してもらうことにより、ブリッジ認証局CA_{bridge}との間で相互認証を行っているものとする。このようにすることで、あるセキュリティドメインＳＤに属する認証局ＣＡと他のセキュリティドメインＳＤに属する認証局ＣＡとの間に、一方の認証局ＣＡが発行した公開鍵証明書の有効性を、他方の認証局ＣＡにて確認できるようにするためのパスが形成される。

【００２４】

次に、上記のＰＫＩシステムを構成するエンドエンティティＥＥ、認証局ＣＡおよび証明書有効性確認センタＶＣについて説明する。

【００２５】

まず、エンドエンティティＥＥについて説明する。

【００２６】

図３は、エンドエンティティＥＥの概略構成を示す図である。

【００２７】

図示するように、エンドエンティティＥＥは、処理部１０ａと、記憶部１０ｂと、ネットワークＮＥＴを介して他装置と通信を行うための通信部１６と、ユーザが作成した電子文書や他のエンドエンティティＥＥあるいはユーザ端末から受け取った電子文書の入出力やユーザよりの指示の受付けを行う入出力部１７と、を有する。

【００２８】

処理部１０ａは、署名生成部１４と、署名検証部１５と、エンドエンティティＥＥの各部を統括的に制御する制御部１８と、を有する。

【００２９】

記憶部１０ｂは、ユーザが作成した（エンドエンティティＥＥが受付サーバの場合はユーザ端末から受け取った）電子文書を保持する電子文書保持部１１と、秘密鍵（署名鍵）とこれに対の公開鍵証明書とを保持する鍵保持部１２と、他のエンドエンティティＥＥから受け取った署名付きの電子文書と公開鍵証明書を保持する検証対象保持部１３と、を有する。

【００３０】

このような構成において、制御部１８は、入出力部１７を介してユーザから、電子文書保持部１１に保持してある電子文書を他のエンドエンティティＥＥに送信すべき旨の指示を受け付けると、当該電子文書を電子文書保持部１１から読み出し、これを署名生成部１４に渡す。これを受けて、署名生成部１４は、鍵保持部１２に保持されている秘密鍵を用いて当該電子文書に対する署名を生成する。それから、制御部１８は、電子文書保持部１１から読み出した電子文書に署名生成部１４で生成された署名を付して、署名付き電子文書を作成する。そして、作成した署名付き電子文書に鍵保持部１２に保持されている公開鍵証明書を添付して、通信部１６を介して、ユーザより指示された送信先のエンドエンティティＥＥのアドレスへ送信する。

【００３１】

また、制御部１８は、通信部１６を介して、他のエンドエンティティＥＥから署名付き電子文書と公開鍵証明書を受け取ると、これらを検証対象保持部１３に保持させると共に、その旨を署名検証部１５に通知する。これを受けて、署名検証部１５は、検証対象保持部１３に保持されている署名付き電子文書の署名を、当該電子文書と共に受け取った公開鍵証明書を用いて検証する。そして、検証が成立した場合にのみ、署名付き電子文書を正当なものとして扱い、必要に応じて入出力部１７から出力する。

【００３２】

ただし、上記の署名検証が成立した場合でも、当該署名検証に用いた公開鍵証明書が、自エンドエンティティＥＥを収容する（つまり、自エンドエンティティＥＥに対して公開鍵証明書を発行した）端末収容認証局ＣＡ以外の端末収容認証局ＣＡの場合は、証明書有効性確認センタＶＣに、上記の署名検証に用いた公開

鍵証明書の有効性の確認依頼を送信する。この際、必要に応じて、前記署名付き電子文書により行おうとしている電子手続の取引額等で示した信頼度（ポリシー）を、前記確認依頼に含める。そして、証明書有効性確認センタＶＣにて、当該公開鍵証明書の有効性が確認された場合にのみ、署名付き電子文書を正当なものとして扱い、必要に応じて入出力部１７から出力する。

【００３３】

次に、認証局ＣＡについて説明する。

【００３４】

図４は、認証局ＣＡの概略構成を示す図である。

【００３５】

図示するように、認証局ＣＡは、処理部２０ａと、記憶部２０ｂと、ネットワークＮＥＴを介して他装置と通信を行うための通信部２６と、公開鍵証明書等の入出力やユーザよりの指示の受付けを行う入出力部２７と、を有する。

【００３６】

処理部２０ａは、公開鍵証明書を発行する発行部２１と、発行部２１が発行した公開鍵証明書の管理を行う管理部２２と、認証局ＣＡの各部を統括的に制御する制御部２８と、を有する。

【００３７】

記憶部２０ｂは、発行部２１が発行した公開鍵証明書を保持する公開鍵証明書データベース２３と、公開鍵証明書データベース２３に保持されている各公開鍵証明書の発行先が記述された発行先管理リストを保持する発行先管理リスト保持部２４と、失効証明書リスト保持部２５と、を有する。

【００３８】

このような構成において、制御部２８は、入出力部２７あるいは通信部２６を介して、公開鍵証明書の発行依頼を受け付けると、その旨を発行部２１に伝える。これを受けて、発行部２１は、発行依頼主が署名生成に用いる秘密鍵（署名鍵）とこれに対の公開鍵証明書を作成する。この際、自認証局ＣＡの秘密鍵で公開鍵証明書に署名をする。また、必要に応じて、公開鍵証明書中に、当該公開鍵証明書の有効期限や、信頼しない他の認証局の名称（Name Constrains）や、当該

公開鍵証明書の有効性確認のために許容される最大パス長（パス上の許容最大認証局数）や、電子手続の取引額等で表した当該公開鍵証明書と対の秘密鍵による署名の信頼度（ポリシー）を記述する。そして、作成した公開鍵証明書と秘密鍵を、入出力部２７あるいは通信部２６を介して、郵送あるいは通信により、発行依頼主に渡す。また、この公開鍵証明書を公開鍵証明書データベース２３に登録すると共に、その発行先（つまり発行依頼主）の情報を、発行先管理リスト保持部２４に保持されている発行先管理リストに記述する。

【００３９】

また、制御部２８は、入出力部２７あるいは通信部２６を介して、公開鍵証明書の失効依頼を受け付けると、その旨を管理部２２に伝える。これを受けて、管理部２２は、失効対象の公開鍵証明書を公開鍵証明書データベース２３から削除すると共に、当該公開鍵証明書の発行先の情報を、発行先管理リスト保持部２４に保持されている発行先管理リストから削除する。そして、管理部２２は、失効依頼により公開鍵証明書データベース２３から削除した公開鍵証明書に関する情報が記述された失効証明書リスト（一般に、ＣＲＬ（Certification Revocation List）、ＡＲＬ（Authority Revocation List）と呼ばれている）を、定期的に作成し、これを失効証明書リスト保持部２５に保持させる。なお、管理部２２は、作成した失効証明書リストに、次回の失効証明書リストの作成予定日時を記述するものとする。

【００４０】

また、制御部２８は、通信部２６を介して、他装置より公開鍵証明書の失効情報の問い合わせを受け取ると、失効証明書リスト保持部２５に保持されている失効証明書リストを検索して、問い合わせのあった公開鍵証明書が失効しているか否かを調べる。そして、その結果を、通信部２６を介して、問い合わせをした他装置に応答する（このような問い合わせと応答に用いる通信プロトコルとして、ＯＳＣＰ（Online Certification status protocol）がある）。

【００４１】

なお、管理部２２は、公開鍵証明書データベース２３に格納されている各公開鍵証明書の有効期限を調査し、有効期限を過ぎている公開鍵証明書を公開鍵証明

書データベース２３から削除すると共に、当該公開鍵証明書の発行先の情報を、発行先管理リスト保持部２４に保持されている発行先管理リストから削除する処理も行う。

【００４２】

次に、証明書有効性確認センタＶＣについて説明する。

【００４３】

図５は、証明書有効性確認センタＶＣの概略構成を示す図である。

【００４４】

図示するように、証明書有効性確認センタＶＣは、処理部３０ａと、記憶部３０ｂと、ネットワークＮＥＴを介して他装置と通信を行うための通信部３６と、公開鍵証明書等の入出力やユーザよりの指示の受付けを行う入出力部３７と、を有する。

【００４５】

処理部３０ａは、パス検索部３２と、パス検証部３３と、有効期限/失効状態調査部３４と、有効性確認部３５と、証明書有効性確認センタＶＣの各部を統括的に制御する制御部３８とを有する。また、記憶部３０ｂは、パスデータベース３１と、失効証明書リスト作成予定日時データベース３９とを有する。

【００４６】

パス検索部３１は、定期的に、ブリッジ認証局CA_{bridge}からエンドエンティティＥＥに対して公開鍵証明書を発行した各端末収容認証局ＣＡまでのパスを検索する。

【００４７】

パス検証部３２は、パス検索部３１でパスの検索が行われる毎に、当該パス検索部３１で検出されたパスの検証を行う。そして、検証が成立したパスを、証明書有効性確認センタＶＣを上流とした場合に当該パス上の最下流に位置することとなる端末収容認証局ＣＡの名称と、当該パス上の各認証局ＣＡから入手した当該パス上の１つ下流側に位置する認証局ＣＡ（発行元の認証局ＣＡが端末収容認証局ＣＡの場合はエンドエンティティＥＥ）に対して発行した公開鍵証明書とに対応付けて、パスデータベース３１に登録する。

【００４８】

有効期限/失効状態調査部３４は、パスデータベース３１に登録されているパス各々について、当該パス上の各認証局ＣＡが当該パス上の１つ下流側に位置する認証局ＣＡ（発行元の認証局ＣＡが端末収容認証局ＣＡの場合はエンドエンティティＥＥ）に対して発行した公開鍵証明書の有効期限や失効の有無を調査する。そして、その結果に応じてパスデータベース３３を更新する。

【００４９】

また、有効期限/失効状態調査部３４は、各認証局ＣＡの失効証明書リスト保持部２５から入手した失効証明書リストに記述されている次回の失効証明書リスト作成予定日時を当該認証局ＣＡに対応付けて、失効証明書リスト作成予定日時データベース３９に登録する。

【００５０】

有効性確認部３５は、エンドエンティティＥＥからの依頼に従い、当該エンドエンティティＥＥを収容する端末収容認証局ＣＡ以外の端末収容認証局ＣＡが発行した公開鍵証明書の、当該エンドエンティティＥＥを収容する端末収容認証局ＣＡに対する有効性の確認を行う。

【００５１】

なお、図３～図５に示すエンドエンティティＥＥ、認証局ＣＡおよび証明書有効性確認センタＶＣの各々は、例えば、図６に示すような、ＣＰＵ６１と、メモリ６２と、ハードディスク等の外部記憶装置６３と、ＣＤ-ＲＯＭ等の可搬性を有する記憶媒体６９から情報を読み取る読取装置６４と、ネットワークを介して他装置と通信を行うための通信装置６５と、キーボードやマウス等の入力装置６６と、モニタやプリンタ等の出力装置６７と、これらの各装置間のデータ送受を行うインターフェース６８とを備えた、一般的な電子計算機において、ＣＰＵ６１がメモリ６２上にロードされた所定のプログラムを実行することにより、実現できる。すなわち、通信部１６、２６、３６は、ＣＰＵ６１が通信装置６６を利用することにより、入出力部１７、２７、３７は、ＣＰＵ６１が入力装置６６や出力装置６７や読取装置６４を利用することにより、そして、記憶部１０ｂ、２０ｂ、３０ｂは、ＣＰＵ６１がメモリ６２や外部記憶装置６３を利用することに

より実現される。また、処理部１０ａ、２０ａ、３０ａは、ＣＰＵ６１上のプロセスとして実現される。

【００５２】

このような、電子計算機上にエンドエンティティＥＥ、認証局ＣＡおよび証明書有効性確認センタＶＣを各々実現するための所定のプログラムは、読取装置６４を介して記憶媒体６９から読み出され、あるいは、通信装置６６を介してネットワーク経由で他のサーバからダウンロードされて、一旦、外部記憶装置６３に格納された後、そこからメモリ６２上にロードされて、あるいは、外部記憶装置６３に格納されることなく、直接メモリ６２上にロードされて、ＣＰＵ６１に実行されるようにすればよい。

【００５３】

次に、上記構成の証明書有効性確認センタＶＣの動作について説明する。

【００５４】

本実施形態の証明書有効性確認センタＶＣの動作は、パスの検索、検証および管理動作と、公開鍵証明書の有効性の確認動作とに分かれる。

【００５５】

まず、パスの検索・検証および管理動作について説明する。

【００５６】

図７～図８は、本実施形態の証明書有効性確認センタＶＣで行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【００５７】

制御部３８は、所定時間（例えば１日）を経過すると（ステップＳ１００１）、パス検索部３２にパス検索を依頼する。これを受けて、パス検索部３２は、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスを検索する（ステップＳ１００２）。

【００５８】

具体的には、パス検索部３２は、ブリッジ認証局CA_{bridge}の発行先管理リスト保持部２４にアクセスし、ブリッジ認証局CA_{bridge}が発行した公開鍵証明書の発行先の情報を入手する。そして、入手した各発行先が認証局ＣＡの場合は、

各発行先の認証局ＣＡの発行先管理リスト保持部２４にアクセスして、各認証局ＣＡが発行した公開鍵証明書の発行先をさらに調べる。この処理を、公開鍵証明書の発行先がエンドエンティティＥＥとなるまで続けることにより、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスを検索する。ここで、パスのループにより上記の処理が無限に繰り返されるのを防止するため、ある認証局ＣＡの発行先管理リスト保持部２４から入手した発行先に、それまでに形成された部分パスの上流側に位置する認証局ＣＡが含まれる場合は、当該認証局ＣＡを発行先とした上記の処理を行わないものとする。

【００５９】

ステップＳ１００２でのパス検索処理を、各認証局ＣＡが図２に示す関係にある場合を例に取り、より具体的に説明する。

【００６０】

まず、パス検索部３２は、ブリッジ認証局CA_{bridge}の発行先管理リスト保持部２４にアクセスし、ブリッジ認証局CA_{bridge}が発行した公開鍵証明書の発行先の情報として、認証局CA_{11}、CA_{21}、CA_{31}の情報を入手する。

【００６１】

次に、パス検索部３２は、ブリッジ認証局CA_{bridge}から入手した発行先（認証局CA_{11}、CA_{21}、CA_{31}）のうちのいずれか１つに注目して、以下の処理を実行する。

【００６２】

すなわち、注目した発行先が認証局ＣＡ（以下、注目認証局ＣＡと呼ぶこととする）であるならば、ブリッジ認証局CA_{bridge}-注目認証局ＣＡ間に、ブリッジ認証局CA_{bridge}側を上流とする部分パスを設定する。そして、注目認証局ＣＡの発行先管理リスト保持部２４にアクセスして、当該注目認証局ＣＡが発行した公開鍵証明書の発行先の情報をさらに入手する。ここでは、注目した発行先が認証局CA_{11}であるとして、ブリッジ認証局CA_{bridge}-認証局CA_{11}間に部分パスを設定し、認証局CA_{11}から、発行先の情報として、認証局CA_{bridge}、CA_{12}、CA_{13}の情報を入手したものとする。

【００６３】

次に、パス検索部３２は、認証局CA_{11}から入手した発行先（認証局CA_{bridge}、CA_{12}、CA_{13}）に、部分パス上の認証局ＣＡ（以下、ループ認証局ＣＡと呼ぶこととする）が含まれているか否かを調べる。含まれている場合はその発行先を注目対象から除外する。したがって、ここでは、認証局CA_{bridge}を注目対象から除外することになる。次に、パス検索部３２は、認証局CA_{11}から入手した発行先にエンドエンティティＥＥが含まれるか否を調べる。エンドエンティティＥＥが含まれている場合、認証局CA_{11}は端末収容認証局となる。しかし、認証局CA_{11}から入手した発行先にエンドエンティティＥＥは含まれていない。したがって、ブリッジ認証局CA_{bridge}-認証局CA_{11}間に設定した部分パスを、端末収容認証局ＣＡまで延長すべく、認証局CA_{11}から入手した、ループ認証局ＣＡを除く発行先（認証局CA_{12}、CA_{13}）のうちのいずれか１つに注目する。

【００６４】

注目した発行先が認証局ＣＡであるならば、それまでに設定した部分パスの下流側にこの注目認証局ＣＡを接続した部分パスを設定する。そして、この注目認証局ＣＡの発行先管理リスト保持部２４にアクセスして、当該注目認証局ＣＡが発行した公開鍵証明書の発行先の情報をさらに入手する。ここでは、注目した発行先が認証局CA_{12}であるとして、ブリッジ認証局CA_{bridge}-認証局CA_{11}-認証局CA_{12}間に部分パスを設定し、認証局CA_{12}から、発行先の情報として、エンドエンティティEE_1、EE_2を入手したものとする。

【００６５】

次に、パス検索部３２は、認証局CA_{12}から入手した発行先（EE_1、EE_2）に、ループ認証局ＣＡが含まれているか否かを調べる。含まれている場合はその発行先を注目対象から除外する。ここでは、ループ認証局ＣＡは含まれないので、パス検索部３２は、次の処理へ移行し、端末収容認証局CA_{12}から入手した発行先にエンドエンティティＥＥが含まれるか否を調べる。ここで、入手した発行先はすべてエンドエンティティＥＥであるので、認証局CA_{12}は端末収容認証局である。そこで、この認証局CA_{12}を最下流とする部分パスを、ブリッジ認証局CA_{bridge}から端末収容認証局CA_{12}までのパス（CA_{bridge}-CA_{11}-CA_{12}）として検出する。

【００６６】

次に、パス検索部３２は、検出したパス上の最下流側に位置する認証局CA_{12}から入手した発行先の情報の中に、未だ注目していない発行先（ループ認証局ＣＡ以外の認証局ＣＡ）があるか否かを調べ、そのような発行先があれば、これを注目認証局ＣＡとして、上記の処理を続ける。一方、そのような発行先がなければ、１つ上流側に位置する認証局CA_{11}から入手した発行先の情報の中に、未だ注目していない発行先（ループ認証局ＣＡ以外の認証局ＣＡ）があるか否かを調べる。そして、そのような発行先があれば、これを注目認証局ＣＡとして、上記の処理を続ける。ここでは、認証局CA_{11}から入手した発行先の情報のうち、認証局CA_{13}について未だ注目していないので、これを注目認証局ＣＡとして上記の処理を行うことにより、ブリッジ認証局CA_{bridge}から端末収容認証局CA_{13}までのパス（CA_{bridge}-CA_{11}-CA_{13}）を検出する。

【００６７】

このように、パス検索部３２は、上記の処理を、検出したパス上に位置する全ての認証局ＣＡ各々について、当該認証局ＣＡから入手した発行先の情報の中に、未だ注目していない発行先（ループ認証局ＣＡ以外の認証局ＣＡ）がなくなるまで続けることにより、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスを検出する。その結果、各認証局ＣＡが図２に示す関係にある場合、パス検索部３２により検出される、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスは、図９に示すとおりとなる。

【００６８】

さて、制御部３８は、パス検索部３２によりブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスが検出されると、パス検証部３３にパスの検証を依頼する。これを受けて、パス検証部３３は、パス検索部３２により検出されたパスの検証を行う（ステップＳ１００３）。

【００６９】

具体的には、パス検索部３２により検出されたパス各々について、以下の処理を行う。

【００７０】

すなわち、まず、パス検証部３３は、パス上の各認証局ＣＡの公開鍵証明書データベース２３にアクセスし、各認証局ＣＡが当該パス上の１つ下流側に位置する認証局ＣＡ（アクセス先認証局ＣＡが端末認証局ＣＡの場合はエンドエンティティＥＥ）に対して発行した公開鍵証明書を入手する。

【００７１】

次に、パス検証部３３は、パスの最下流に位置する端末収容認証局ＣＡが発行した公開鍵証明書の署名を、１つ上流側の認証局ＣＡが発行した公開鍵証明書で検証し、検証が成立した場合は当該１つ上流側の認証局ＣＡが発行した公開鍵証明書の署名をさらに１つ上流側の認証局ＣＡが発行した公開鍵証明書で検証する。この処理を、当該１つ上流側の認証局ＣＡがブリッジ認証局CA_{bridge}となるまで続けることにより、当該パスを仮検証する。

【００７２】

例えば、図２においてブリッジ認証局CA_{bridge}から端末収容認証局CA_{13}までのパス（CA_{bridge}-CA_{11}-CA_{13}）を仮検証する場合、まず、端末収容認証局CA_{13}が発行した公開鍵証明書の署名を、端末収容認証局CA_{13}より１つ上流側の認証局ＣＡであるルート認証局CA_{11}が端末収容認証局CA_{13}に対して発行した公開鍵証明書を用いて検証する。そして、検証が成立した場合は、ルート認証局CA_{11}が発行した公開鍵証明書の署名を、ルート認証局CA_{11}より１つ上流側の認証局ＣＡであるブリッジ認証局CA_{bridge}がルート認証局CA_{11}に対して発行した公開鍵証明書を用いて検証する。そして、この検証が成立した場合に、ブリッジ認証局CA_{bridge}から端末収容認証局CA_{13}までのパスの仮検証が成立したものとする。

【００７３】

次に、パス検証部３３は、パスの仮検証が成立したならば、当該パス上の各認証局ＣＡから入手した公開鍵証明書中に、信頼しない他の認証局の名称（Name Constrains）や当該公開鍵証明書の有効性確認のために許容される最大パス長（パス上の許容最大認証局数）などの制限の記述があるか否かを調べる。そのような記述がある場合は、当該パスがその制限を満たしているか否かを調べ、満たしている場合にのみ、当該パスの検証が成立したものとする。

【００７４】

例えば、図２においてブリッジ認証局CA_{bridge}から端末収容認証局CA_{26}までのパス（CA_{bridge}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26}）の仮検証が成立した場合において、認証局CA_{26}から入手した公開鍵証明書中に信頼しない他の認証局の名称として認証局CA_{31}が記述されている場合、当該パスの検証は成立しなかったものとする。また、上記の場合において、認証局CA_{26}から入手した公開鍵証明書中にパス長として認証局数＝５が記述されている場合、当該パスの検証は成立しなかったものとする。

【００７５】

さて、制御部３８は、上記のようにして、パス検索部３２により検出されたパス各々に対するパス検証部３３での検証が終了したならば、パスデータベース３１の登録内容を一旦クリアし、それから、パス検証部３３での検証が成立したパス各々を、当該パス上の最下流に位置する端末収容認証局ＣＡと、当該パス上の各認証局ＣＡから入手した公開鍵証明書とに対応付けて、パスデータベース３１に登録する（ステップＳ１００４）。

【００７６】

一方、有効期限/失効状態調査部３４は、パスデータベース３１に登録されている公開鍵証明書の中に、有効期限切れの公開鍵証明書があるか否かを調べる（ステップＳ１００５）。有効期限切れの公開鍵証明書がある場合は、当該公開鍵証明書の発行元認証局ＣＡの公開鍵証明書データベース２３にアクセスして、当該公開鍵証明書の発行先に対して新たに発行された公開鍵証明書を検索する（ステップＳ１００６）。

【００７７】

そして、そのような公開鍵証明書が前記発行元認証局ＣＡの公開鍵証明書データベース２３中になければ、前記有効期限切れの公開鍵証明書に対応付けて登録されているパスに関する情報をパスデータベース３１から削除する（ステップＳ１００７）。一方、そのような公開鍵証明書が前記発行元認証局ＣＡの公開鍵証明書データベース２３中にあればこれを入手する。そして、前記有効期限切れの公開鍵証明書に対応付けてパスデータベース３１に登録されているパスの検証を

、当該有効期限切れの公開鍵証明書の代わりに新たに入手した公開鍵証明書を用いて、上記のステップＳ１００３と同じ要領で行う（ステップＳ１００８）。

【００７８】

なお、ステップＳ１００８でのパス検証に代えて、新たに入手した公開鍵証明書の署名を、当該パス上において、当該公開鍵証明書の発行元認証局ＣＡより１つ上流側に位置する認証局ＣＡが発行した公開鍵証明書で検証し、検証が成立した場合に、当該パスの検証が成立したものとして扱うようにしてもよい。

【００７９】

さて、パスの検証が成立した場合（ステップＳ１００９でＹｅｓ）は、当該パスに対応付けられてパスデータベース３１に登録されている前記有効期限切れの公開鍵証明書を、新たに入手した公開鍵証明書に置き換える（ステップＳ１０１０）。一方、パスの検証が成立しなかった場合（ステップＳ１００９でＮｏ）は、前記有効期限切れの公開鍵証明書に対応付けて登録されているパスをパスデータベース３１から削除する（ステップＳ１０１１）。

【００８０】

次に、有効期限/失効状態調査部３４は、失効証明書リスト作成予定日時データベース３９を調べ、既に経過した失効証明書リスト作成予定日時に対応付けられている認証局ＣＡを検索する（ステップＳ１０１２）。そのような認証局ＣＡが存在する場合（ステップＳ１０１３でＹｅｓ）は、当該認証局ＣＡの失効証明書リスト保持部２５にアクセスして、当該認証局ＣＡが発行した最新の失効証明書リストを入手する（ステップＳ１０１４）。そして、失効証明書リスト作成予定日時データベース３９にて、当該認証局ＣＡに対応付けて登録されている失効証明書リスト作成予定日時を、入手した最新の失効証明書リストに記述されている失効証明書リスト作成予定日時に更新する（ステップＳ１０１５）。

【００８１】

それから、有効期限/失効状態調査部３４は、入手した最新の失効証明書リストに記述されている公開鍵証明書が、パスデータベース３１に登録されているか否かを調べ（ステップＳ１０１６）、登録されている場合は、当該公開鍵証明書に対応付けられているパスに関する情報をパスデータベース３１から削除する（

ステップＳ１０１７）。

【００８２】

次に、公開鍵証明書の有効性の確認動作について説明する。

【００８３】

図１０～図１１は、本実施形態の証明書有効性確認センタＶＣで行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【００８４】

制御部３８は、通信部３６を介して、エンドエンティティＥＥから、少なくとも当該エンドエンティティＥＥを収容する端末収容認証局ＣＡの名称を含んだ、当該端末収容認証局ＣＡ以外の端末収容認証局ＣＡが発行した公開鍵証明書の有効性の確認依頼を受け取ると（ステップＳ２００１）、その旨を有効性確認部３５に通知する。

【００８５】

これを受けて、有効性確認部３５は、依頼対象の公開鍵証明書の記述から特定される当該証明書を発行した端末収容認証局ＣＡに対応付けられたパスと、依頼主のエンドエンティティＥＥを収容する端末収容認証局ＣＡに対応付けられたパスとが、パスデータベース３１に登録されているか否かを調べる（ステップＳ２００２）。

【００８６】

その結果、依頼対象の公開鍵証明書を発行した端末収容認証局ＣＡに対応付けられたパス、および、依頼主のエンドエンティティＥＥを収容する端末収容認証局ＣＡに対応付けられたパスの両方が、パスデータベース３１に登録されていないことが判明したならば、有効性確認部３５は、公開鍵証明書が有効でない旨を、通信部３６を介して、依頼主のエンドエンティティＥＥに通知する（ステップＳ２００３）。

【００８７】

一方、依頼対象の公開鍵証明書を発行した端末収容認証局ＣＡに対応付けられたパス、および、依頼主のエンドエンティティＥＥを収容する端末収容認証局ＣＡに対応付けられたパスの両方が、パスデータベース３１に登録されていること

が確認できたならば、有効性確認部３５は、これら２つのパスのいずれかに対応付けられてパスデータベース３１に登録されている各公開鍵証明書中に、信頼しない他の認証局の名称（Name Constrains）や当該公開鍵証明書の有効性確認のために許容される最大パス長（パス上の許容最大認証局数）などの制限の記述があるか否かをさらに調べる（ステップＳ２００４）。

【００８８】

そのような制限の記述がない場合、ステップＳ２００６に移行する。一方、そのような制限の記述がある場合は、ステップＳ２００５に移行して、これら２つのパスがその制限を満たしているか否か、すなわち、各公開鍵証明書中に、これら２つのパス上のいずれかの認証局を信頼しない旨が記述されているか否か、および、最大パス長として、これら２つのパス上の認証局数よりも少ない認証局数が記述されているか否かを調べる。

【００８９】

そして、そのような記述がある場合、有効性確認部３５は、これら２つのパスがその制限を満たしていないものと判断し、公開鍵証明書が有効性でない旨を、通信部３６を介して、依頼主のエンドエンティティＥＥに通知する（ステップＳ２００３）。一方、そのような記述がない場合は、これら２つのパスがその制限を満たしているものと判断し、ステップＳ２００６に移行する。

【００９０】

ステップＳ２００６では、有効性確認部３５は、エンドエンティティＥＥから受け取った確認依頼に、当該エンドエンティティＥＥが行おうとしている電子手続の取引額等で示された信頼度（ポリシー）が含まれているか否かを調べる。電子手続の信頼度が含まれている場合は、これら２つのパスのいずれかに対応付けられてパスデータベース３１に登録されている各公開鍵証明書中に、前記電子手続の信頼度よりも低い信頼度の記述があるか否かをさらに調べる（ステップＳ２００７）。

【００９１】

そして、そのような記述がある場合は、これら２つのパスを、依頼主のエンドエンティティＥＥが行おうとしている電子手続のための公開鍵証明書の有効性確

認に利用できないものと判断し、公開鍵証明書が有効でない旨を、通信部３６を介して、依頼主のエンドエンティティＥＥに通知する（ステップＳ２００３）。

【００９２】

一方、エンドエンティティＥＥから受け取った確認依頼に当該エンドエンティティＥＥが行おうとしている電子手続の信頼度が含まれていない場合、あるいは、含まれていても、これら２つのパスのいずれかに対応付けられてパスデータベース３１に登録されている各公開鍵証明書中に記述されている信頼度が前記電子手続の信頼度よりも高い場合は、公開鍵証明書は有効であると判断し、公開鍵証明書が有効である旨を、通信部３６を介して、依頼主のエンドエンティティＥＥに通知する（ステップＳ２００８）。

【００９３】

以上、本発明の第１実施形態について説明した。

【００９４】

本実施形態では、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスの検索および検証を、エンドエンティティＥＥからの公開鍵証明書の有効性確認依頼とは独立して、定期的に行うようにしている。そして、あるエンドエンティティＥＥから公開鍵証明書の有効性確認依頼を受けた場合、予め検索、検証したパスを用いて、当該エンドエンティティＥＥを収容する端末収容認証局ＣＡと依頼対象の公開鍵証明書を発行した端末収容認証局ＣＡとの間に、ブリッジ認証局CA_{bridge}を介したパスを構築することができるか否かを調べることで、当該公開鍵証明書が有効であるか否かを判断するようにしている。したがって、公開鍵証明書の有効性確認依頼を受けてから、当該有効性を確認するまでにかかる時間を短縮することができる。

【００９５】

また、本実施形態では、あるエンドエンティティＥＥから公開鍵証明書の有効性確認依頼を受けた場合、予め検索、検証したパスを用いて、当該エンドエンティティＥＥを収容する端末収容認証局ＣＡと依頼対象の公開鍵証明書を発行した端末収容認証局ＣＡとの間に、ブリッジ認証局CA_{bridge}を介したパスを構築することができるか否かを調べ、できた場合に、当該パス上の認証局が発行した公

開鍵証明書中に記述された制限（信頼しない他の認証局の名称（Name Constrains）や最大パス長（パス上の許容最大認証局数）や信頼度（ポリシー）等）を考慮して、依頼対象の公開鍵証明書が有効であるか否かを最終的に判断するようにしている。したがって、公開鍵証明書の有効性確認の判断をより正確に行うことが可能となる。

【００９６】

なお、本発明は、上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【００９７】

例えば、上記の実施形態では、証明書有効性確認センタＶＣは、ブリッジ認証局CA_{bridge}を起点認証局とし、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスの検索および検証を行うようにしている。しかし、本発明はこれに限定されない。他の任意の認証局ＣＡを起点認証局として、各端末収容認証局ＣＡまでのパスの検索および検証を行うこともできる。例えば、各認証局ＣＡが図２に示す関係にある場合、各セキュリティドメインＳＤのルート認証局CA_{11}、CA_{21}、CA_{31}のいずれかを起点認証局として、各端末収容認証局ＣＡまでのパスの検索および検証を行うようにしてもよい。

【００９８】

また、上記の実施形態では、説明をわかりやすくするため、図２に示すように、端末収容認証局ＣＡはエンドエンティティＥＥに対してのみ公開鍵証明書を発行し、その他の認証局ＣＡは認証局ＣＡに対してのみ公開鍵証明書を発行するものとしているが、本発明は、当然のことながら、エンドエンティティＥＥと認証局ＣＡの両方に対して公開鍵証明書を発行するような認証局ＣＡを含む場合でも、同様に適用できる。

【００９９】

【発明の効果】

以上説明したように、本発明によれば、公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮することができる。

【図面の簡単な説明】

【図１】

本発明の一実施形態が適用されたＰＫＩシステムの概略構成を示す図である。

【図２】

図１に示すＰＫＩシステムでの各認証局ＣＡの関係の一例を示す図である。

【図３】

図１に示すエンドエンティティＥＥの概略構成を示す図である。

【図４】

図１に示す認証局ＣＡの概略構成を示す図である。

【図５】

図１に示す証明書有効性確認センタＶＣの概略構成を示す図である。

【図６】

図３～図５に示すエンドエンティティＥＥ、認証局ＣＡおよび証明書有効性確認センタＶＣの各々のハードウエア構成例を示す図である。

【図７】

図５に示す証明書有効性確認センタＶＣで行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【図８】

図５に示す証明書有効性確認センタＶＣで行われるパスの検索、検証および管理動作を説明するためのフロー図である。

【図９】

各認証局ＣＡが図２に示す関係にある場合に、証明書有効性確認センタＶＣのパス検索部３２で検出される、ブリッジ認証局CA_{bridge}から各端末収容認証局ＣＡまでのパスを示す図である。

【図１０】

図５に示す証明書有効性確認センタＶＣで行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【図１１】

図５に示す証明書有効性確認センタＶＣで行われる公開鍵証明書の有効性の確認動作を説明するためのフロー図である。

【図１２】

従来のＰＫＩにおいて、認証局が複数ある場合における各認証局の関係の一例を示す図である。

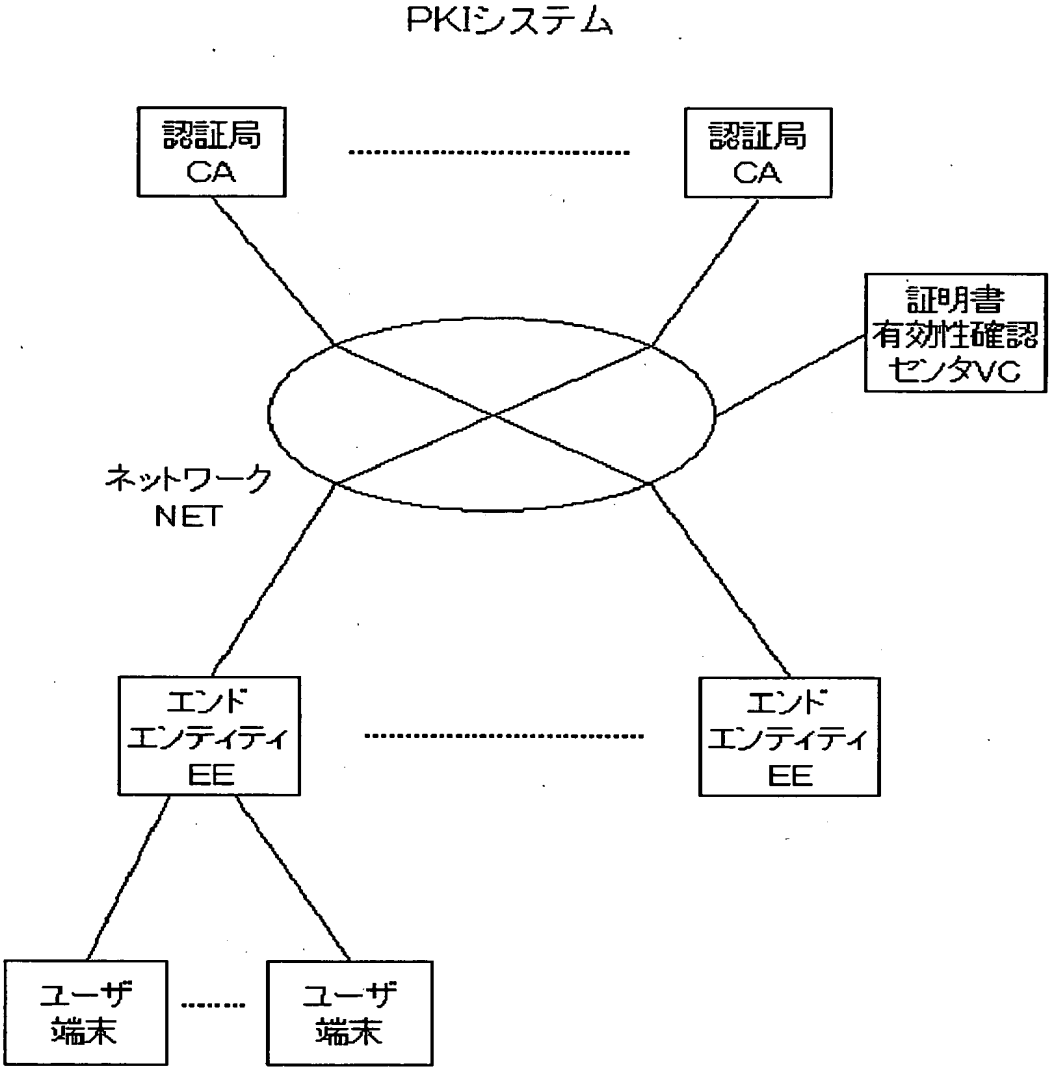
【符号の説明】

ＣＡ…認証局、ＶＣ…証明書有効性確認センタ、ＥＥ…エンドエンティティ、ＳＤ…セキュリティドメイン、１０ａ，２０ａ，３０ａ…処理部、１０ｂ，２０ｂ，３０ｂ…記憶部、１１…電子文書保持部、１２…鍵保持部、１３…検証対象保持部、１４…署名生成部、１５…署名検証部、１６，２６，３６…通信部、１７，２７，３７…入出力部、１８，２８，３８…制御部、２１…発行部、２２…管理部、２３…公開鍵証明書データベース、２４…発行先リスト保持部、２５…失効証明書リスト保持部、３１…パスデータベース、３２…パス検索部、３３…パス検証部、３４…有効期限/失効状態調査部、３５…有効性確認部、３９…失効証明書リスト作成予定日時データベース、６１…ＣＰＵ、６２…メモリ、６３…外部記憶装置、６４…読取装置、６５…通信装置、６６…入力装置、６７…出力装置、６８…インターフェース、６９…記憶媒体

【書類名】図面

【図１】

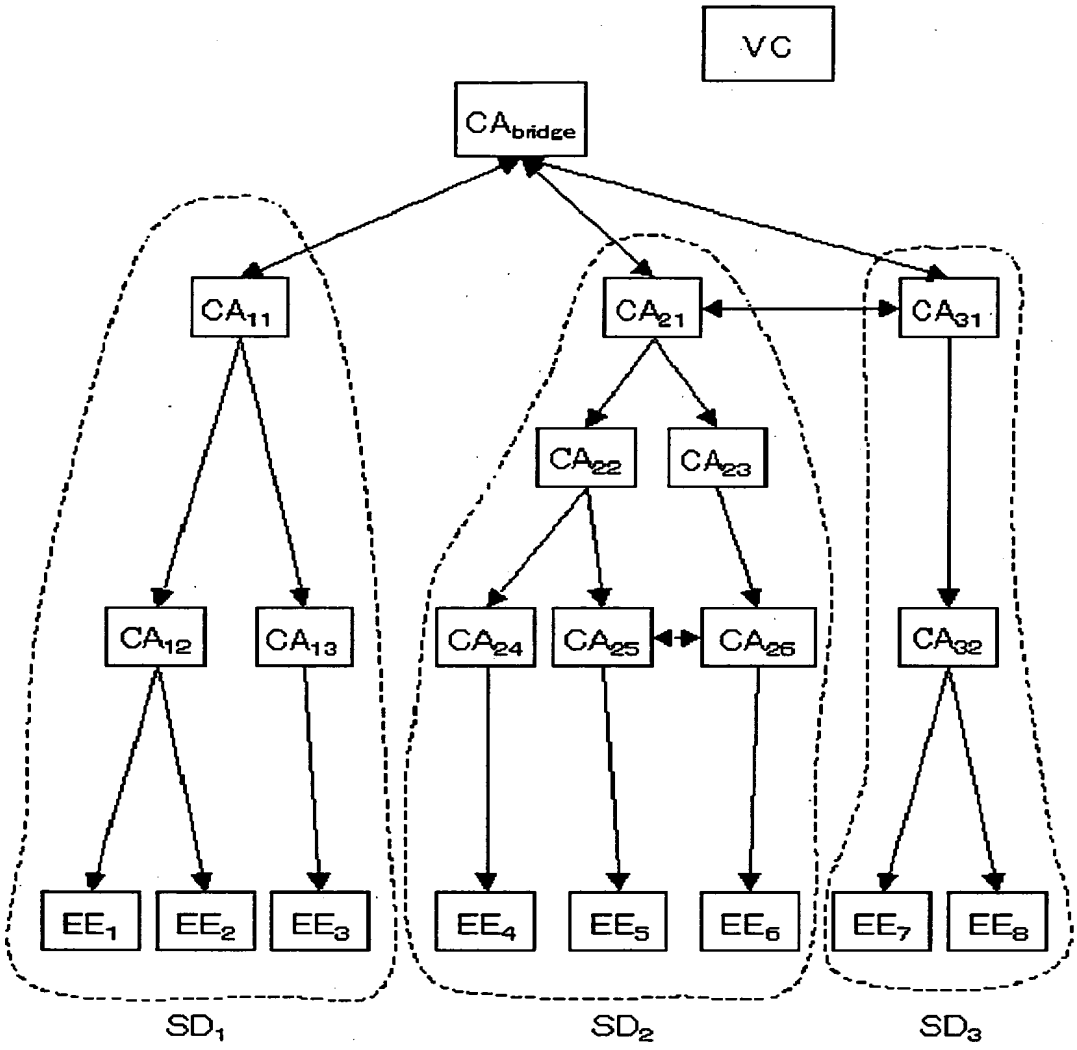
図1



出証特２００１－３０７９４６８

【図２】

図2



⟶ ：公開鍵証明書の流れ

CA：認証局

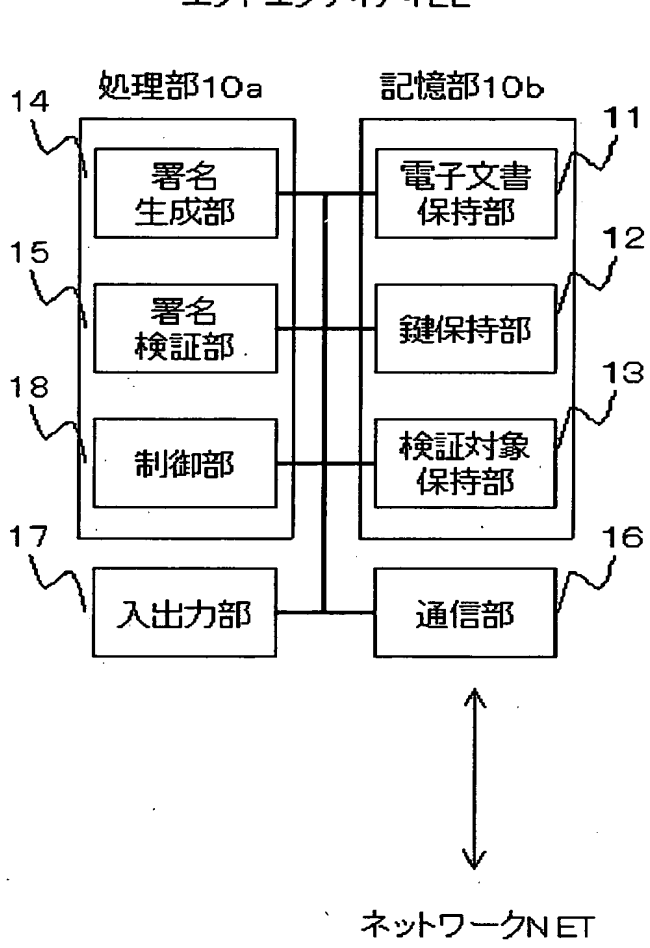
EE：エンドエンティティ

VC：証明書有効性確認センタ

SD：セキュリティドメイン

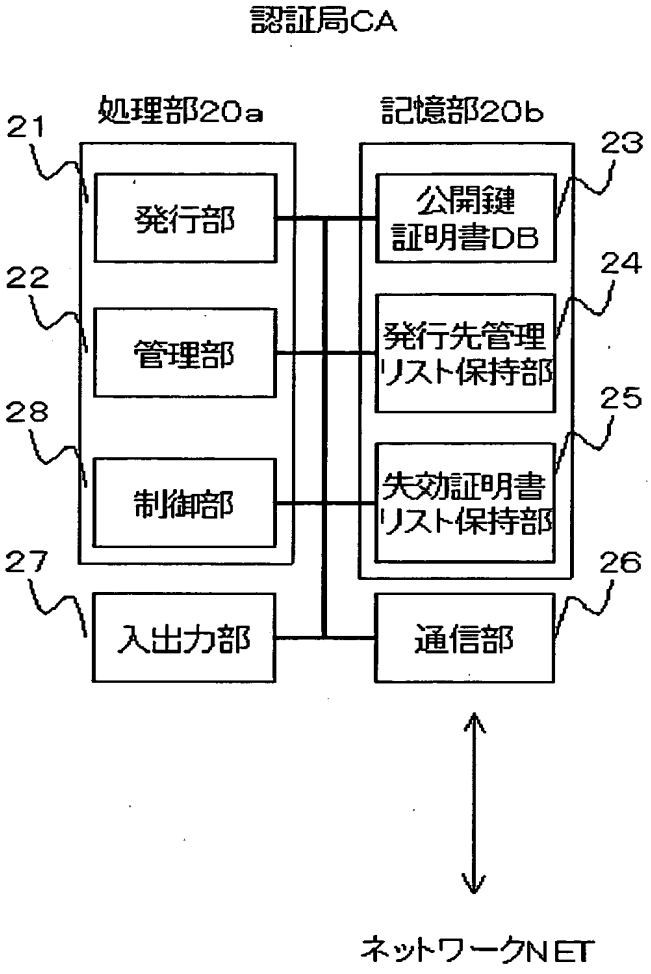
【図３】

図3


エンドエンティティEE
処理部10a
記憶部10b
14
署名
生成部
15
署名
検証部
18
制御部
17
入出力部
11
電子文書
保持部
12
鍵保持部
13
検証対象
保持部
16
通信部
ネットワークNET

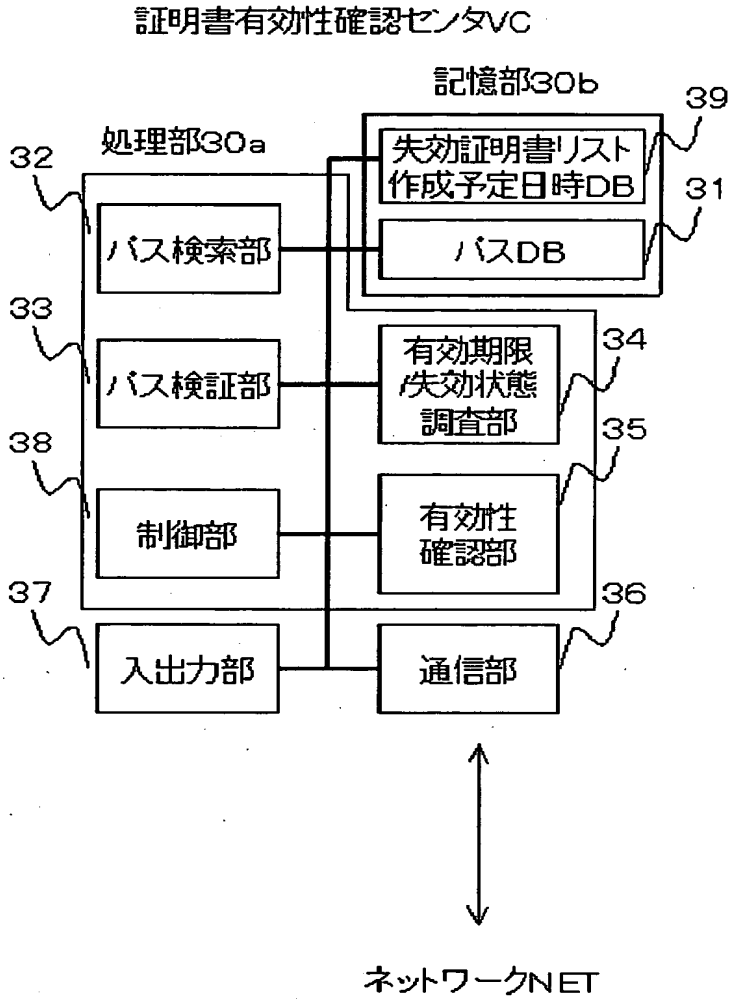
【図４】

図4


認証局CA
処理部20a
記憶部20b
21
22
28
27
23
24
25
26
発行部
管理部
制御部
入出力部
公開鍵
証明書DB
発行先管理
リスト保持部
失効証明書
リスト保持部
通信部
ネットワークNET

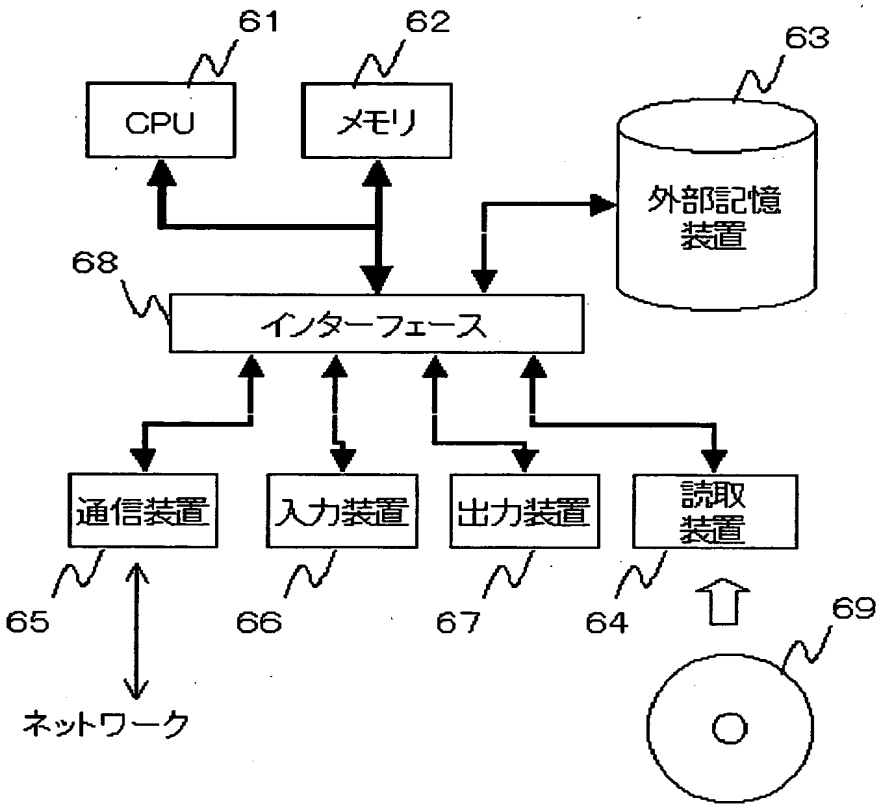
【図５】

図５


証明書有効性確認センタVC
記憶部30b
39
処理部30a
32
失効証明書リスト
作成予定日時DB
31
パス検索部
パスDB
33
パス検証部
有効期限
/失効状態
調査部
34
35
38
制御部
有効性
確認部
37
36
入出力部
通信部
ネットワークNET

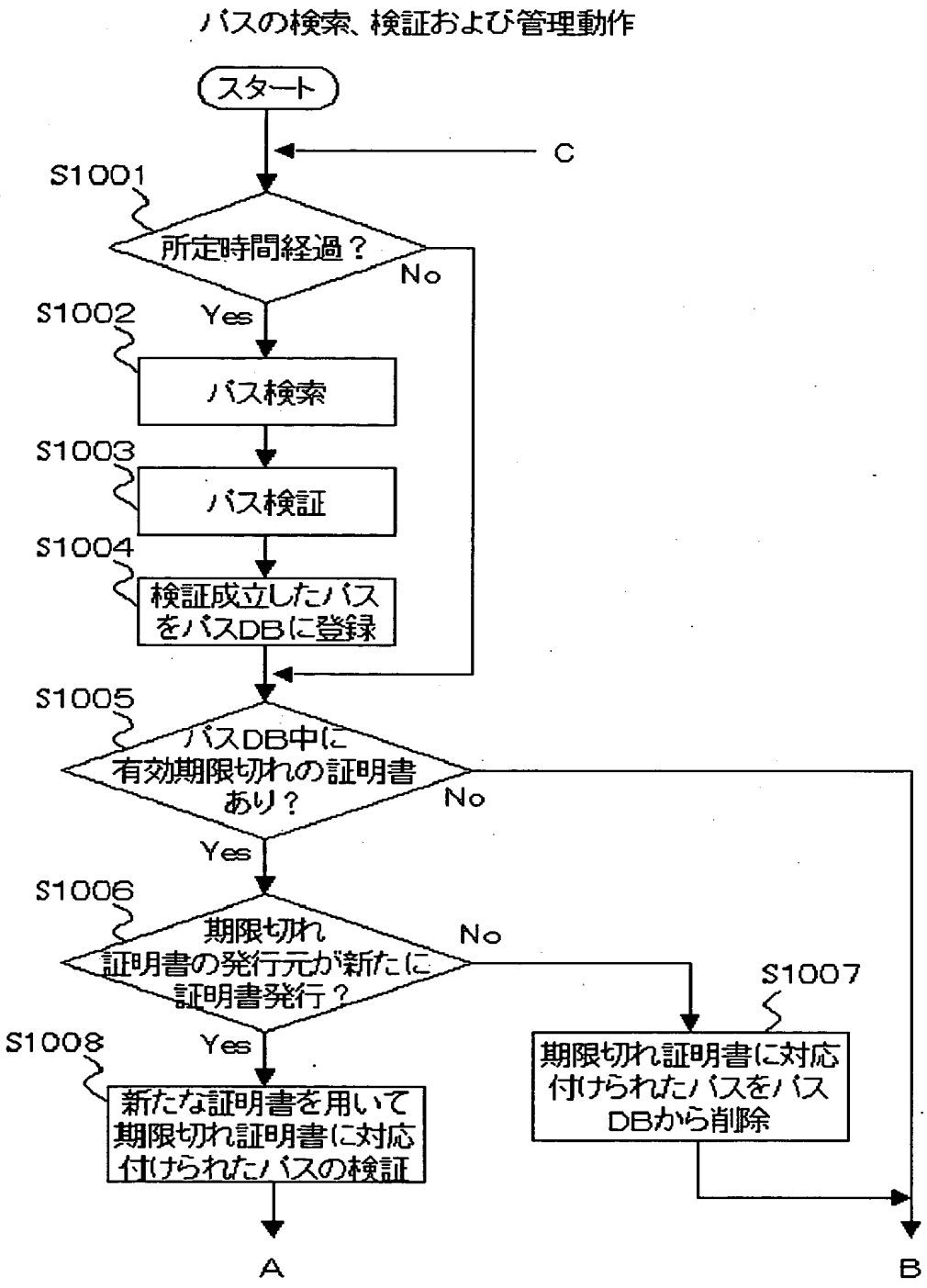
【図6】

図6


61
62
63
CPU
メモリ
外部記憶装置
68
インターフェース
通信装置
入力装置
出力装置
読取装置
65
66
67
64
69
ネットワーク

【図7】

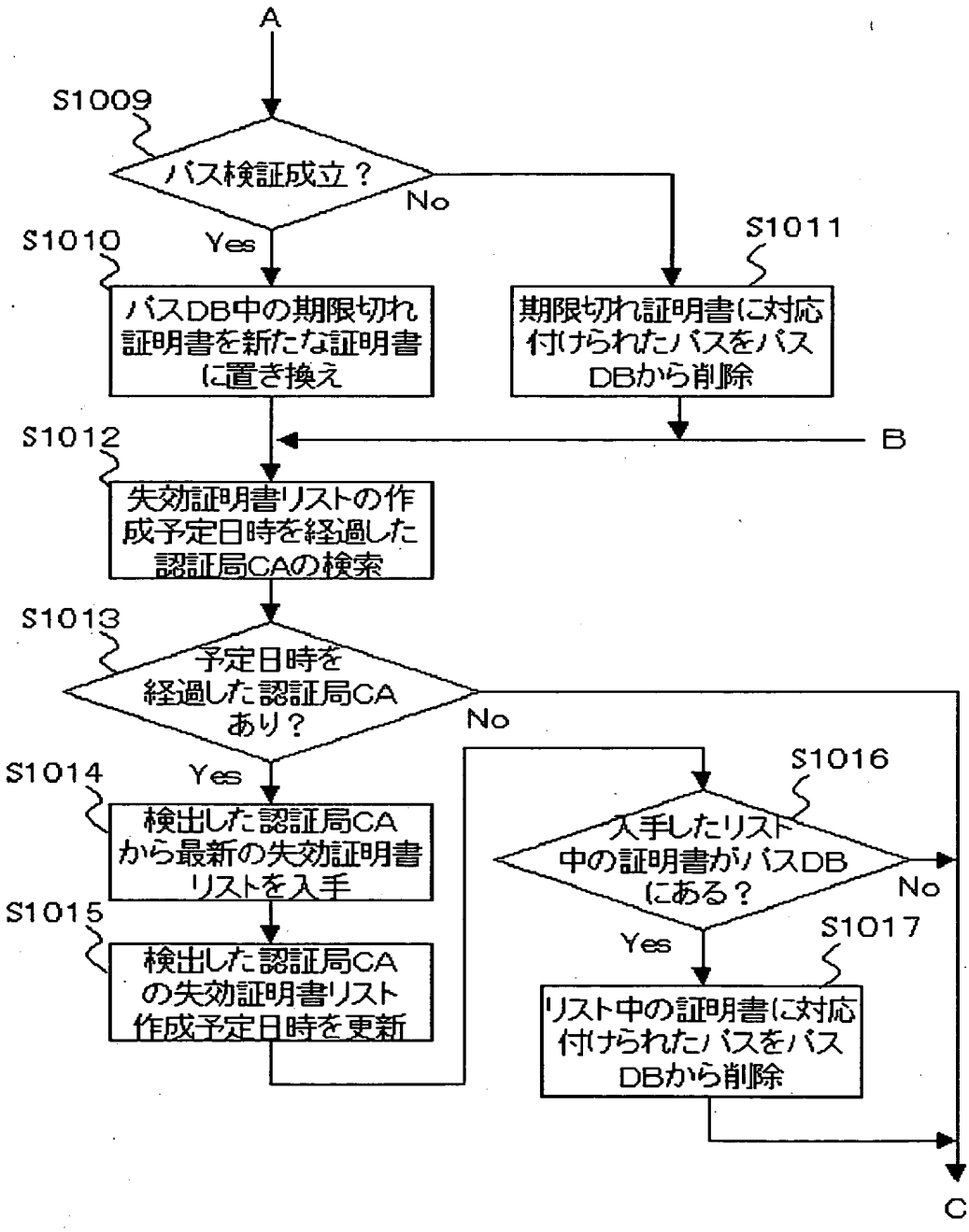
図7


パスの検索、検証および管理動作
スタート
C
S1001
所定時間経過？
No
Yes
S1002
パス検索
S1003
パス検証
S1004
検証成立したパス
をパスDBに登録
S1005
パスDB中に
有効期限切れの証明書
あり？
No
Yes
S1006
期限切れ
証明書の発行元が新たに
証明書発行？
No
S1007
期限切れ証明書に対応
付けられたパスをパス
DBから削除
S1008
Yes
新たな証明書を用いて
期限切れ証明書に対応
付けられたパスの検証
A
B

【図８】

図8

パスの検索、検証および管理動作



【図９】

図9

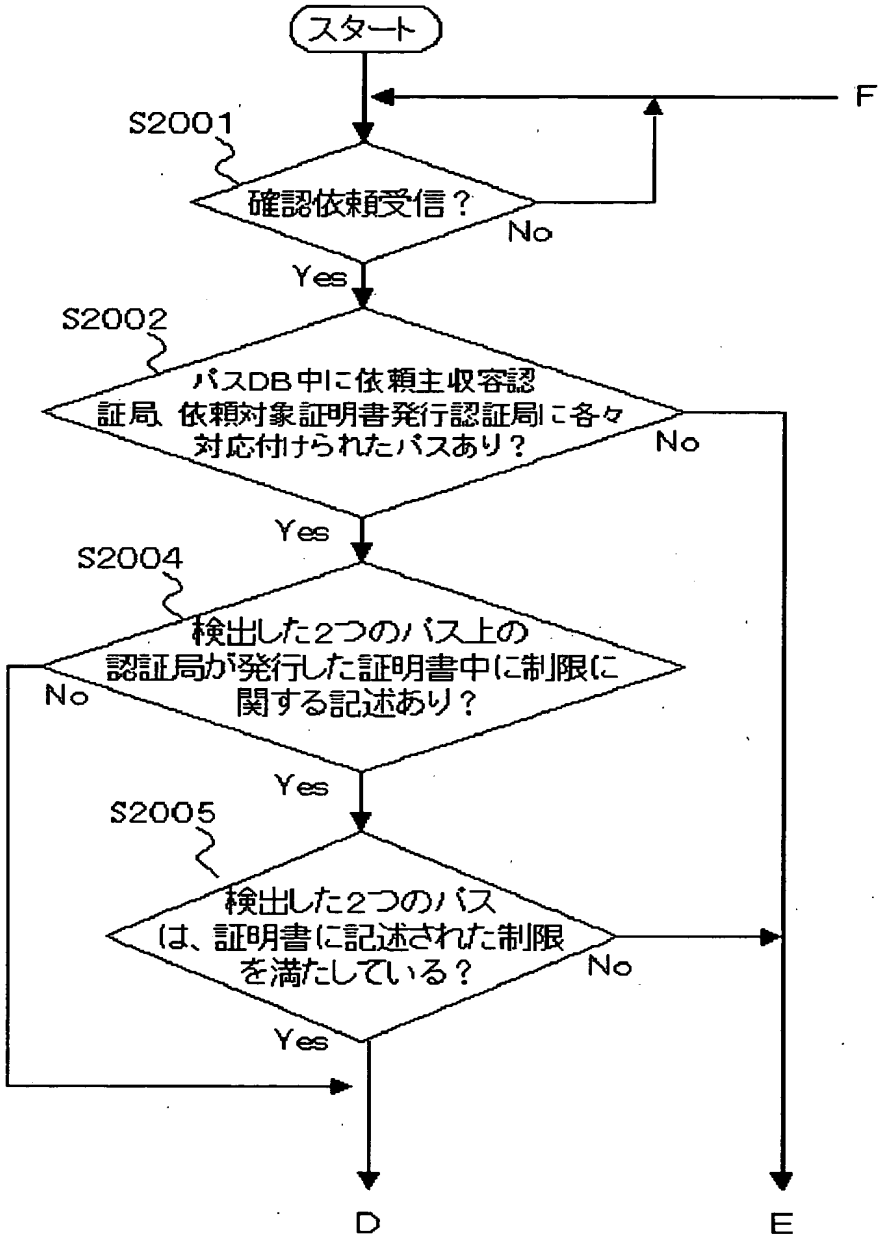
パス検索結果(図2の場合)

端末収容認証局	パス
CA_{12}	CA_{bride}-CA_{11}-CA_{12}
CA_{13}	CA_{bride}-CA_{11}-CA_{13}
CA_{24}	CA_{bride}-CA_{21}-CA_{22}-CA_{24}
	CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{24}
CA_{25}	CA_{bride}-CA_{21}-CA_{22}-CA_{25}
	CA_{bride}-CA_{21}-CA_{23}-CA_{26}-CA_{25}
	CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{25}
	CA_{bride}-CA_{31}-CA_{21}-CA_{23}-CA_{26}-CA_{25}
CA_{26}	CA_{bride}-CA_{21}-CA_{23}-CA_{26}
	CA_{bride}-CA_{21}-CA_{22}-CA_{25}-CA_{26}
	CA_{bride}-CA_{31}-CA_{21}-CA_{23}-CA_{26}
	CA_{bride}-CA_{31}-CA_{21}-CA_{22}-CA_{25}-CA_{26}
CA_{32}	CA_{bride}-CA_{31}-CA_{32}
	CA_{bride}-CA_{21}-CA_{31}-CA_{32}

【図１０】

図10

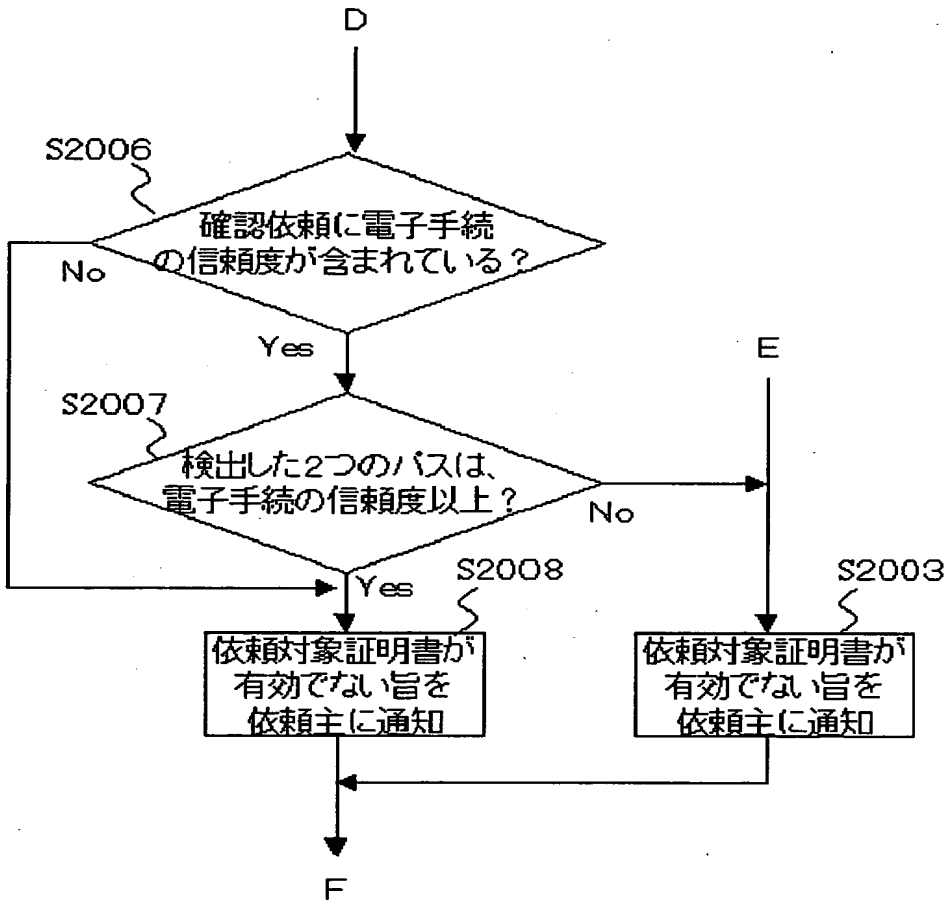
公開鍵証明書の有効性の確認動作



【図１１】

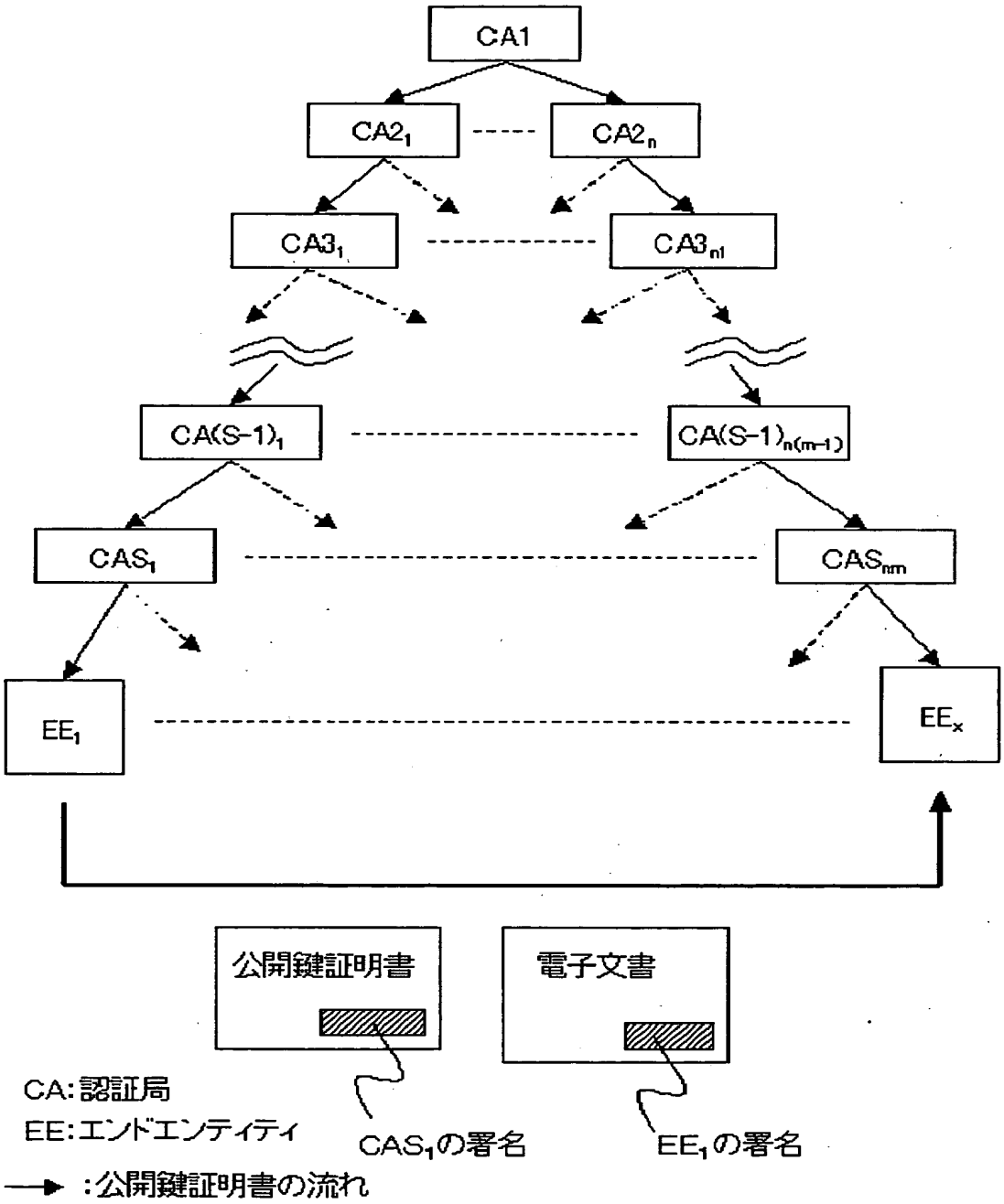
図11

公開鍵証明書の有効性の確認動作



【図１２】

図12


CA1
CA2₁
CA2n
CA3₁
CA3n1
CA(S-1)₁
CA(S-1)n(m-1)
CAS₁
CASnm
EE₁
EEx
公開鍵証明書
電子文書
CA:認証局
EE:エンドエンティティ
CAS₁の署名
EE₁の署名
:公開鍵証明書の流れ

【書類名】要約書

【要約】

【課題】公開鍵証明書の有効性確認を依頼してから、当該有効性が確認されるまでにかかる時間を短縮する。

【解決手段】証明書有効性確認センタＶＣは、ブリッジ認証局$ＣＡ_{bridge}$から各端末認証局ＣＡまでのパスの検索、検証を定期的に行い、検証が成立したパスを端末収容認証局に対応付けてパスＤＢに登録する。また、エンドエンティティＥＥから証明書の有効性確認依頼があった場合、当該エンドエンティティＥＥを収容する端末収容認証局ＣＡに対応付けられたパスと依頼対象証明書を発行した端末収容認証局ＣＡに対応付けられたパスとがパスＤＢに登録されているか否かを調べ、両者が登録されている場合にのみ、当該証明書は有効であると判断する。

【選択図】図２

出証特２００１－３０７９４６８

出願人履歴情報

識別番号　〔000005108〕

1．変更年月日　1990年　8月31日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台4丁目6番地
氏　名　株式会社日立製作所